Smart Technology. Delivered.

Testing Wi-Fi Functionality in Medical Devices

Originally Published: October 2013

A White Paper from Laird Technologies

Applications on many medical devices require secure and persistent network connections. Hospitals present challenges to reliable Wi-Fi connectivity.

To ensure reliable functionality, a Wi-Fi radio that is embedded in a medical device must be tested thoroughly. But where, and how?

Americas: +1-800-492-2320 Option 3
Europe: +44-1628-858-940
Hong Kong: +852-2268-6567 x026
www.lairdtech.com/wireless

Contents

TESTING FOR KEY REQUIREMENTS

Wi-Fi® access in a hospital serves different sets of users and applications. Patients and guests use Wi-Fi for convenient Internet access from smartphones, tablets, and laptops. Clinicians and administrators use Wi-Fi to gain access to hospital networks from personal computing devices such as smartphones or from hospital-managed computing devices such as workstations on wheels and tablet computers. And, increasingly, computing devices are sharing the hospital Wi-Fi airwaves with medical devices.

Medical devices place stringent requirements on Wi-Fi connections. Many medical devices run applications that require a persistent network connection, because a disruption of even a tenth of a second (100 milliseconds) can cause a failure in the transmission of a continuous stream of data. Radio frequency (RF) transmissions between the medical device and an infrastructure endpoint, called an access point (AP), may be absorbed by lead walls or human bodies, redirected by metal objects and surfaces, or disrupted by sources of RF interference.

In addition to RF performance, key requirements include:

- **Interoperability:** Wi-Fi client devices must interoperate with Wi-Fi infrastructure products. Cisco Systems has the largest share of the Wi-Fi infrastructure market in hospitals, but enterprise-grade infrastructure products from Aruba Networks and other vendors are popular in hospitals, too.
- **Security:** All Wi-Fi connections must be secure so that sensitive information transmitted over the air is protected and access to hospital Wi-Fi networks and the resources behind them is controlled.
- **Mobility:** Persistent network connections over Wi-Fi are required not just by stationary medical devices but also by medical devices that roam from one AP to another.

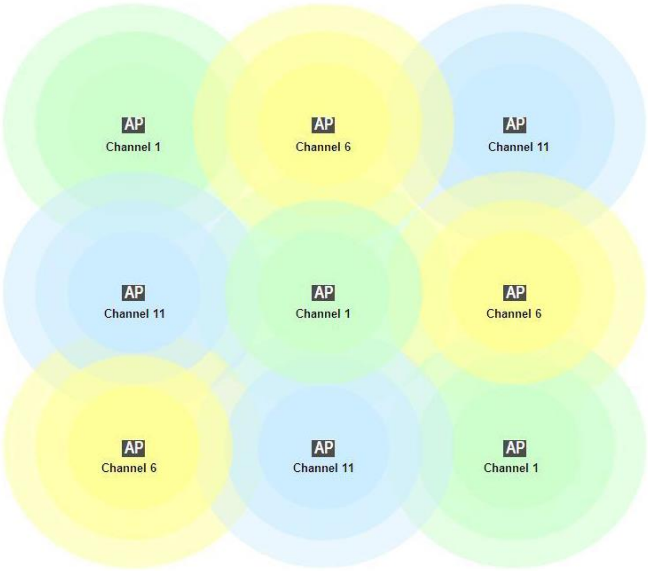
A medical device will address these key requirements if the Wi-Fi radio in that device has the right functionality. That functionality must be verified through testing. Let’s examine some items that must be tested for each key requirement.

RF Performance

Testing the RF characteristics of a Wi-Fi radio includes testing the radio’s compliance with various regulatory requirements, its range, and its ability to handle RF interference. A radio’s RF characteristics are controlled by the radio’s hardware and the antennas to which that hardware is connected. RF testing with one antenna configuration may not be valid with a different antenna configuration. See the section “Reference Device vs. Medical Device” for details.

Different geographic regions of the world are parts of different regulatory domains. When operating in a domain, a Wi-Fi radio must be in compliance with all regulatory requirements for that domain. RF regulatory requirements are determined by bodies such as the Federal Communications Commission (FCC) in the US and Canada, or CE and ETSI in the EU. Compliance is demonstrated by passing a set of tests and earning one or more certificates. While there are some device-level certifications that the medical device manufacturer must obtain, most certifications can and should be obtained by the Wi-Fi radio supplier.

RF range must be tested because coverage patterns in hospitals are inconsistent. A wireless medical device must maintain connectivity to a hospital’s Wi-Fi network, even when no AP offers a strong RF signal. Even when there are overlapping coverage patterns as depicted below, there are some locations where a client device is at the edge of coverage for one AP and not within the coverage area of any other AP. Examples of edge-of-coverage situations in hospitals include corners of the building and elevators. The greater the range of a client device, the better its chances of maintaining connectivity in edge-of-coverage situations.



The transmit power and receive sensitivity of the wireless radio are determinative factors in the range, so both characteristics must be tested. Transmit power is the level of power that the radio generates at the RF interface. This is calculated as the amount of energy produces across a defined frequency bandwidth. Receive sensitivity is essentially the "point of no return:" if the radio receives a signal less than the stated receive sensitivity, it will not read the data.

A client's ability to handle interference must also be tested because hospitals have a significant amount of interference, particularly in the 2.4 GHz band. While interference may not cause a medical device to lose connectivity, it will cause the device to retry its attempts to send and receive data, often numerous times. Sources of RF interference in the 2.4 GHz band include other Wi-Fi devices, Zigbee devices, Bluetooth devices, baby monitors, and cordless phones. These 2.4 GHz interference sources can be avoided if hospitals move their medical devices to the 5 GHz band. (For more information, read our white paper on this topic, here.)

Interoperability with Popular Wi-Fi Infrastructures

For a client device such as a medical device, the Wi-Fi CERTIFIED™ seal signifies that the device interoperates with Wi-Fi infrastructure that also carries the seal. According to the Wi-Fi Alliance®, a client device earns the Wi-Fi CERTIFIED seal if it passes tests "in numerous configurations and with a diverse sampling of [Wi-Fi CERTIFIED infrastructure] equipment…that operates in the same frequency band." The seal, however, does not offer sufficient evidence that a medical device will work well with a hospital's Wi-Fi infrastructure, even if both carry the seal. To understand why, you must understand what tests are and are not included in Wi-Fi CERTIFIED testing.

For each Wi-Fi specification, such as 802.11n, the Wi-Fi Alliance issues a Wi-Fi CERTIFIED test plan. The test plan for a client device (or station) specifies infrastructure devices, such as APs, from three different vendors. When a specification is new, the Wi-Fi Alliance selects the vendors from among those that are first to support for the new specification. If one of the vendors releases a new model of an AP, the Wi-Fi Alliance may replace the AP specified in the test plan with the newer model.

All of the APs in a test plan may be consumer-grade APs and not those in common use in hospitals. Odds are slim that a test plan will include the exact model of AP that a particular hospital uses or even that is popular in hospitals.

More importantly, a Wi-Fi CERTIFIED test plan does not include tests for certain functionality that is relevant and often important to the operation of medical devices in a hospital. Included in a Wi-Fi CERTIFIED test plan are tests for functionality that are specific to the specification (such as 802.11n) and tests for security, which the Wi-Fi Alliance defines as WPA2®. (See the Security section of this white paper for details.) Items not included in a Wi-Fi CERTIFIED test plan but relevant to the operation of medical devices on a hospital network include:

- RF performance (discussed in the previous section)

- Roaming performance
- Stress testing
- Different network scenarios
- Power save modes
- Rate shifting

For a hospital with a Cisco Wi-Fi infrastructure, the Cisco Compatible seal on a medical device provides assurance that the device will interoperate with the Cisco infrastructure. A Wi-Fi client device can earn the Cisco Compatible seal through a program called Cisco Compatible Extensions, or CCX. Like the Wi-Fi Alliance certification program, CCX:

- Includes a specification that defines a set of features that must be implemented in the hardware and software for a Wi-Fi radio or a device that uses a Wi-Fi radio
- Requires compliance testing conducted by an independent lab that is approved by the organization that manages the program
- Requires that a submitted radio or device passes all tests to be approved

Cisco provides specifications and a complete test plan that test engineers must follow when testing their radios for CCX. The CCX program has a structure that is similar to that of the Wi-Fi CERTIFIED test plan. With both programs:

- One or more specifications define what features must be implemented in the hardware and software for a Wi-Fi radio or a device that uses a Wi-Fi radio
- Compliance testing is conducted by an independent lab that is approved by the organization that manages the program
- A device must pass all tests to be certified

The primary differences between the CCX program and the Wi-Fi CERTIFIED test plan are:

- Who manages the program
- What types of devices are eligible for certification testing
- What is in the specification

CCX is part of the Cisco Developer Network (CDN) and is managed by Cisco. The Wi-Fi certification program is managed by the Wi-Fi Alliance. CCX is for client devices that interact with Cisco's enterprise-class wireless LAN infrastructure products, which are used by businesses and other organizations. The Wi-Fi certification program, on the other hand, is for any type of product that uses Wi-Fi technology. CCX targets business client devices and nothing else. The Wi-Fi certification program is much broader, and its specification includes fewer elements than the CCX specification. The CCX specification is, in fact, a superset of the specification used for Wi-Fi compliance. A device cannot be certified as Cisco Compatible unless that device or the Wi-Fi radio that it uses is Wi-Fi CERTIFIED.

Security

Before allowing medical devices to connect to hospital networks using Wi-Fi, those responsible for information security must be confident that the Wi-Fi networks and the medical devices that use them will protect sensitive information, including electronic medical records (EMRs) that are transmitted over Wi-Fi or stored on the networks.

The Wi-Fi industry standard for enterprise-grade security is the Enterprise version of WPA2®, or WPA2-Enterprise. WPA2 is a security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks. WPA2-Enterprise aligns with IEEE 802.11i, the ratified IEEE standard for Wi-Fi security. The Wi-Fi Alliance also defines a consumer-grade version of WPA2, called WPA2-Personal.

Both versions of WPA2 define a process for mutual authentication between the Wi-Fi client and the Wi-Fi infrastructure. At the end of the authentication process, a key is derived dynamically from the information exchanged between the client and the infrastructure. After the authentication process completes, the derived key is used to encrypt and decrypt all unicast data that travels between the client and the infrastructure. The encryption (and decryption) method is AES-CCMP, which is strong enough to be approved by the U.S. federal government for its cryptography standard of FIPS 140-2.

With WPA2-Personal, authentication is done through a four-way handshake using a pre-shared key (PSK) or passphrase. If the PSK on the Wi-Fi client matches the PSK on the AP to which the client is trying to associate, then the authentication succeeds. WPA2-Enterprise authentication relies on IEEE 802.1X, a ratified standard for network access control. 802.1X supports a set of Extensible Authentication Protocol, or EAP, types for mutual authentication of the client device and the network to which it is trying to connect.

While PSKs are easy to implement on small networks, a hacker can "guess" a short PSK using a dictionary attack. To avoid vulnerability to a dictionary attack, a PSK or passphrase must be a random string of at least 20 characters, including characters other than letters and digits. Configuring a complex PSK or passphrase on every client device and AP represents an administrative challenge, one that must be repeated every time a user that knows the PSK or passphrase leaves the organization.

Information security personnel in most hospitals prefer WPA2-Enterprise for all Wi-Fi networks to which medical devices can connect.

While WPA2-Personal authentication relies on a statically configured pre-shared key or passphrase, WPA2-Enterprise authentication relies on IEEE 802.1X, a ratified standard for network access control. 802.1X supports a set of Extensible Authentication Protocol, or EAP, types for mutual authentication of the client device and the network to which it is trying to connect. 802.1X authentication with an EAP type such as PEAP or EAP-TLS is extremely strong. If WPA2-Enterprise authentication succeeds, then an encryption key for the client is derived and stored on the client and the AP.

The table below compares popular EAP types that are used with 802.1X authentication.

Type	Credential(s)	Database(s)	Pros and Cons
LEAP	Microsoft password	Active Directory (AD)	No certificates Strong password required
PEAP with EAP-MSCHAP	Microsoft password	AD	Native support in Windows, CE CA certificate on every client device
PEAP with EAP-GTC	Password, one-time password, token	AD, NDS, LDAP, OTP database	Broad range of credentials CA certificate on every client device
EAP-TTLS	Wide variety	Wide variety	Broad range of credentials Not widely supported
EAP-FAST	Microsoft password, others	AD, others	No certificates Complex provisioning process
EAP-TLS	Client certificate	Certificate authority (CA)	Very strong authentication Native support in Windows, CE CA, user certificates on every client device

A device can earn the Wi-Fi CERTIFIED seal without supporting WPA2-Enterprise; support for WPA2-Personal is sufficient for the seal. Even when it earns the seal for WPA2-Enterprise, the Wi-Fi CERTIFIED test plan does not include tests for every EAP type and every configuration that may be in use at a hospital.

U.S. federal government installations, such as Veterans Administration hospitals, may require a medical device to have a FIPS 140-2 validation. Even though AES-CCMP, the WPA2 encryption algorithm, is sufficient for FIPS 140-2, achieving a FIPS 140-2 validation with WPA2-Enterprise is extremely difficult. To learn why, read our white paper on FIPS 140-2.

Mobility

Providing a persistent Wi-Fi network connection for a stationary medical device can be difficult in a typical hospital. As mentioned earlier, Wi-Fi RF transmissions between the device and an AP may be absorbed by lead walls or human bodies, redirected by metal objects and surfaces, or disrupted by sources of RF interference.

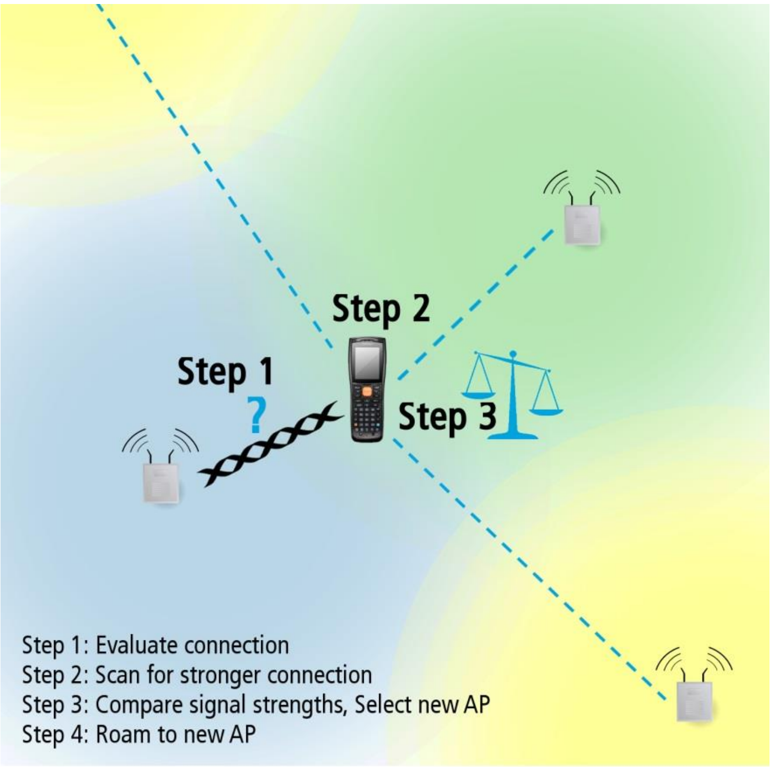
When a medical device is mobile, providing a persistent Wi-Fi network connection for that device is even more challenging. The device may move from a location where it has an unobstructed RF connection with an AP to a second location where the connection with the AP is more tenuous to a third location where the connection is lost.

As soon as a connection becomes suboptimal or tenuous, the device must switch, or roam, from its current AP to another AP. Fast and effective roaming is essential to ensuring persistent network connections and trouble-free operation of the applications that rely on such connections.

In a typical hospital Wi-Fi deployment, a large area is covered by the radio signals of many APs, with each AP offering an area or “cell” of coverage on a particular frequency channel. The coverage area of one AP overlaps with the coverage areas of nearby APs. To minimize co-channel interference – collisions of signals from APs on the same channel – APs with overlapping cells operate on different channels.

When a client device is associated to a nearby AP, the Wi-Fi radio in the client receives a strong signal from the AP. This signal enables the connection between the AP and the client to support a high data rate. As the client moves away from the AP, the strength of the signal decreases and the relative impact of interference sources in the area increases. Sometimes, the transmitted data packets are not received, forcing the sender to retry the transmission. To maintain the reliability of data transfer over the connection, the client and AP negotiate a lower data rate.

If the client device continues to move away from the AP, then it eventually reaches the edge of coverage for that AP, where a connection can be maintained only at the lowest data rate supported by that AP. Beyond the edge of coverage, the client is out of range for that AP, and the connection with the AP is lost. Before losing its connection, the client must switch from the current AP to one that provides better connectivity.


Step 1
?
Step 2
Step 3
Step 1: Evaluate connection
Step 2: Scan for stronger connection
Step 3: Compare signal strengths, Select new AP
Step 4: Roam to new AP

Roaming is more complex than just switching from one AP to another. The roaming process has four distinct steps:

1. **Evaluate:** Determine if the connection with the current AP is less than optimal, typically by examining the strength of the RF signal from the current AP and comparing it to a threshold value.
2. **Scan:** Determine what other APs are in the vicinity by scanning every frequency channel on which an AP may be operating. While a client is scanning, it cannot interact with the AP with which it is connected. The most efficient scan is an active scan, where the client issues a probe request and listens for a probe response from an AP. The alternative to an active scan is a passive scan, where the client listens on each channel for beacons, which APs send out periodically. The risk with a passive scan is that, if the client does not wait long enough on a channel, then the client may miss an AP's beacon. Passive scans must be done on 5 GHz channels where Dynamic Frequency Selection (DFS) is required.
3. **Select:** Select the AP that is most likely to provide a better connection than the current AP.
4. **Roam and Reauthenticate:** Roam from the current AP to the selected AP, and reauthenticate to the (Layer 2) network on which the APs reside. When WPA2-Enterprise is used, reauthentication is 802.1X reauthentication using an EAP type that may involve communication with an authentication server on the network. There are three methods for accelerating EAP reauthentications:
   a. Cisco Centralized Key Management, or CCKM, which is supported by Wi-Fi infrastructure products from Cisco and by clients that are certified for CCX
   b. Opportunistic Pairwise Master Key (OPMK) caching, which is supported with WPA2 by some controller-based Wi-Fi infrastructures and by some clients
   c. IEEE 802.11r pre-authentication, which is not widely supported today

Where To Test

Hospitals

If you want to determine how the Wi-Fi embedded in a medical device will perform in a hospital, then the most obvious place to test is in that hospital. After all, the RF propagation characteristics, AP coverage patterns, infrastructure devices and software versions, client device mix, and other Wi-Fi characteristics of a hospital usually are unique to that hospital.

It may not be viable, however, to conduct thorough medical device Wi-Fi tests in a hospital. Because medical devices provide patient care, they operate in areas of the hospital where patients receive care. Patient care is, of course, the main function of hospitals, and hospitals are averse to introducing risk into patient care areas.

Most hospitals view Wi-Fi tests as an activity that introduces risk, and so that activity is forbidden or tightly restricted in patient care areas.

Even when Wi-Fi testing is allowed in a hospital, no one on the hospital's staff may have the time and expertise to conduct thorough tests on each medical device. The maker of a medical device may have both, but conducting Wi-Fi tests on a medical device in every hospital that is interested in the device is a daunting proposition for even the largest medical device maker.

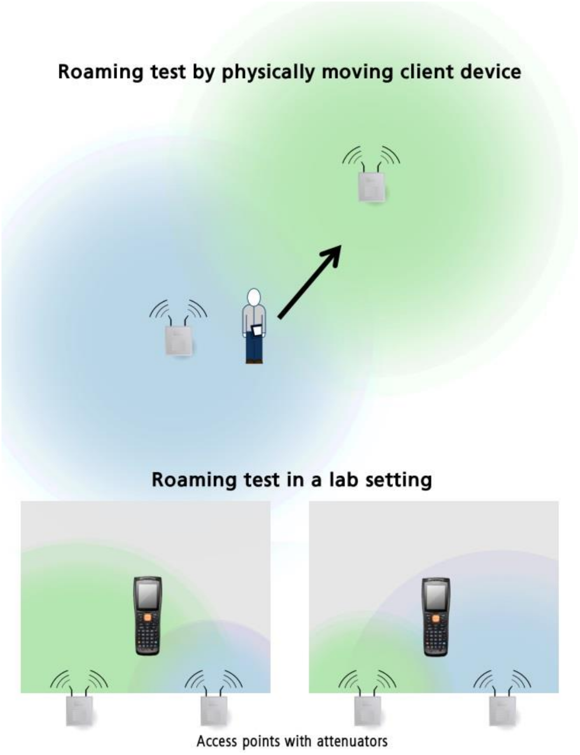
Other Environments

Because conducting tests of medical device Wi-Fi in hospitals can be difficult or impossible, medical device makers sometimes conduct tests in more accessible environments that are meant to simulate a hospital. APs in an office building, warehouse, or other structure can be deployed and configured to have coverage patterns similar to those seen in a portion of a hospital. Medical devices then can be tested in that "hospital-like" environment.

Two challenges of testing in a "hospital-like" environment are (1) deploying and configuring APs from different manufacturers and (2) simulating the RF characteristics of a hospital. Wireless functionality should be tested on a variety of infrastructure from different providers. For each brand of wireless infrastructure the test site must perform a complete site survey. This is both costly and time-consuming. Also, other characteristics of hospitals are difficult to recreate, such as lead walls, interference from a variety of devices, and people constantly walking around. It is difficult to recreate all of these characteristics in a "hospital-like" environment.

A Lab

In a controlled lab environment, it is possible to simulate many of the RF characteristics of a hospital, such as materials that absorb RF transmissions, materials that reflect RF transmissions (resulting in multipath interference), interference from other Wi-Fi clients, and other sources of RF interference. One key advantage of a lab is that you can use APs and other Wi-Fi infrastructure gear from different vendors without having to mount the APs in the ceiling.


Roaming test by physically moving client device
Roaming test in a lab setting
Access points with attenuators

To be effective at simulating "real world" conditions, a test lab requires specialized test equipment:

- A **packet analyzer** (also known as a packet sniffer) is used to intercept and log, or packet capture, traffic passing over a network. A packet analyzer is an extremely versatile test tool that can be used to monitor the conditions of the test environment, attempt to read and decode traffic in the environment, and identify the effects of interference on the tested device.
- A **shield room** protects precision equipment from the influence of external magnetic fields or electromagnetic signals that might interfere with the testing of a device.
- An **attenuator** is an electronic device that reduces

the power of a signal without appreciably distorting its waveform. An attenuator is effectively the opposite of an amplifier, though the two work by different methods. While an amplifier provides gain, an attenuator provides loss, or gain less than 1.

In the roaming test described in the previous section, the test is done by physically moving the client device so it must jump from AP to AP. In a lab environment, test engineers can recreate the process of roaming. Using an attenuator to increase and decrease the wireless signal from a stationary AP, a lab can trick the client device into thinking it is actually moving closer or further away from the AP, causing it to roam. Testing in a lab can be difficult, but when set up properly it is the most efficient and most effective way to test Wi-Fi.

Staff and Automation

Regardless of where tests are conducted, they must be performed by a well-trained staff that follows proven methods and processes to ensure that tests are valid and test results are analyzed thoroughly.

When all tests are conducted manually, the volume of tests can overwhelm a limited staff. To maximize the tests that a limited staff can perform, you must automate the tests. Equipment that automates Wi-Fi tests is specialized and expensive, and customizing that equipment can require many hours of diligent effort.

HOW TO TEST

Reference Client vs. Medical Device

There are several differences and issues between performing Wi-Fi testing on the actual customer medical device as opposed to performing Wi-Fi testing on a generic reference client device. One main physical characteristic of the two unique devices that can possibly lead to different RF performance between them is the antenna. Both the antenna selection and physical placement of the antenna within the device can impact RF performance. Every type of antenna has different characteristics, such as unique gain and propagation patterns. If the customer's device contains an antenna that is different than the tested device, with different characteristics, the RF performance might be different. The physical placement of the antenna within the two devices might also impact performance. Different physical locations within each of the devices might produce interference to receiving the radio signal.

Other physical parts of the wireless device might cause another problem known as multipath propagation. Multipath propagation occurs when a single radio transmission encounters a reflective material (such as metal) and then duplicates into multiple transmissions in the same way that a sound wave can echo when it encounters reflective objects. Multipath propagation typically reduces the performance of 802.11a, 802.11b, and 802.11g- compliant devices that support only single spatial streams because duplicate transmissions can be perceived by the receiving radio as original transmissions (which must be processed and subsequently discarded). Antenna placement or material composition in either the reference client or the actual device may cause multipath propogation in one device but not the other.

Taking all of these issues into consideration, it is preferable for medical device manufacturers to make sure that their wireless module providers are able to test their actual device as opposed to a reference client device.

Testing RF Performance

RF performance in Wi-Fi radios is dependent on a number of items. RF performance testing must be done to ensure regulatory compliance, determine RF range, and ability to maintain connectivity. .

There are numerous RF regulatory requirements administered by government regulatory bodies like the FCC and ETSI. Regulatory certification testing can be expensive and time consuming for medical device manufacturers; instead, they should choose radio suppliers who provide as many certifications as possible.

Range testing is typically done in an open air environment to determine the maximum possible range of the wireless radio. This is not the best method, instead range testing should be done in a lab environment with the ability to automate and simulate different scenarios. The best way to do interference testing is also in a lab.

Testing Interoperability

Testing Wi-Fi interoperability in a real hospital is next to impossible. It only allows for a glimpse of the functionality of one specific wireless infrastructure from one vendor, such as Cisco, Aruba, or others, with one controller software version, and APs with one specific firmware version. It is also difficult for medical device providers to do interoperability testing on their own because it would be costly to obtain infrastructure from every possible vendor. It is less difficult to do interoperability testing in a lab setting. Labs can more easily set up common infrastructure configurations with the most popular firmware and software versions to complete testing.

Testing Security

Even though WPA2-Enterprise is the preferred approach for Wi-Fi security, not every medical device supports it. As a result, Wi-Fi networks in some hospitals support WPA2-Personal instead of WPA2-Enterprise. Because a medical device vendor often cannot dictate to a hospital what method of Wi-Fi security must be used in the hospital, it is important to test that the Wi-Fi radio in the medical device supports both WPA2-Enterprise and WPA2-Personal. Tests of WPA2-Enterprise support should be conducted with a broad range of EAP types and a range of popular authentication servers such as RADIUS (Remote Authentication Dial-In User Service), the most widely-used protocol for authentication servers. TACACS+ (Terminal Access Controller Access Control System Plus) is a Cisco-developed product that is also popular.

Security tests must ensure that the radio consistently connects to an AP, passes data to the network at expected data rates, receives data from the network at expected data rates, and roams from one AP to another seamlessly. These tests should work regardless of the Wi-Fi infrastructure and the authentication server on the network.

Testing Mobility

Laird Technologies tests for connectivity and roaming in both the 2.4 GHz band and the 5 GHz band. The major difference between radio operation in each of the bands is that the 2.4 GHz band has fewer channels, so scanning for a new AP takes less time, thus roaming is quicker. In addition, the 5 GHz band has dynamic frequency selection (DFS) channels. The use of DFS channels is a mechanism to allow unlicensed devices to use the 5 GHz frequency bands already allocated to radar systems without causing interference to those radars. If an end user device has DFS channels enabled, the scan time increases significantly. Roaming in the 5 GHz band is more challenging because it takes much longer for the radio to roam to find a new AP.

A few ways that Laird Technologies tests radios for connectivity and roaming is by using automated tests and by doing “walk around” tests. Walk around tests are done with a complete infrastructure network set up and a test engineer physically walks around with the wireless device. One specific walk around test is an edge of coverage test. In this test, the wireless devices is walked outside of the network and then moved back into the network to ensure that the radio stays connected to the edge of the network and then reconnects as soon as the radio is back in range. This test simulates operation in a challenging environment.

In addition to this test, Laird does a catastrophic roam test in order to simulate a challenging environment. In a typical "smooth" roam test, the client device experiences gradually decreasing signal strength. In contrast with a smooth roam test, in a catastrophic roam test the client quickly loses connectivity with its associated access point. This test evaluates the time it takes for the Wi-Fi radio to roam and reconnect to an AP. In an ideal situation, the radio will quickly connect to the original AP or a new AP without a break in the data transfer. These and all other roaming and connectivity tests are done with different possible radio settings to ensure that the radio roams and stays connected in all situations in a variety of roam environments.

Conclusion and Recommendations

Medical device manufacturers should choose embedded Wi-Fi radios from manufacturers who have proven test methods. Laird Technologies employs a skilled test team that utilizes a state-of-the-art test lab and has developed proven methods by which to test Wi-Fi radios for use in challenging environments.

Laird Technologies tests for all supported features and characteristics that customers are most concerned with, which include security, connectivity, roaming and specific regulatory certifications such as CCX and Wi-Fi Alliance certifications.